

# Cross Site Scripting

Joshua D. Abraham  
< jabra @ spl0it.org >  
Northeastern University  
October 31, 2008

# Presentation Agenda

- Introduction
- Details of Cross Site Scripting
- Explaining the Attack Vector
- Demo
- Conclusion

# Presentation Agenda

- Introduction
- Details of Cross Site Scripting
- Explaining the Attack Vector
- Demo
- Conclusion

# Web Applications

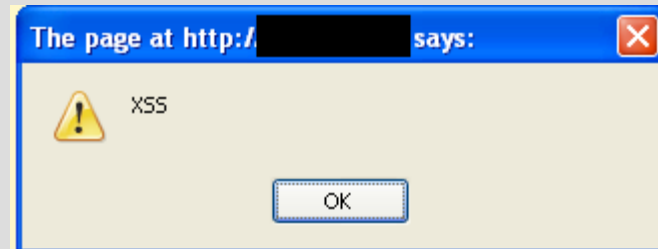
- Presence on the web
- Not your mother's internet
  - Social Networking (facebook, twitter etc)
- Dynamic content

# Presentation Agenda

- Introduction
- [Details of Cross Site Scripting](#)
- Explaining the Attack Vector
- Demo
- Conclusion

# Cross Site Scripting

- What is Cross Site Scripting?
- What are the Types?
  - DOM-Based
  - Reflective
  - Persistent



# Reflective Cross Site Scripting

- Query Reflected on the Page
- Many vectors
  - GET parameters
  - POST parameters
  - Header parameters
- Input from the Browser written to the page

# Persistent Cross Site Scripting

- Storage of Malicious JavaScript in the database
- Example: Administrative Log Page
  - Reads username from DB for a failed login attempt
  - Write the result to the an administrative log
  - ...
  - What if we enter:
    - `<script>alert('XSS')</script>` as the username???
- Input from the DB written to the page



# DOM-Based Cross Site Scripting

- Written to the DOM
- Example:
  - `document.write('<script>alert('XSS')</script>');`
- Input written to the page via Javascript

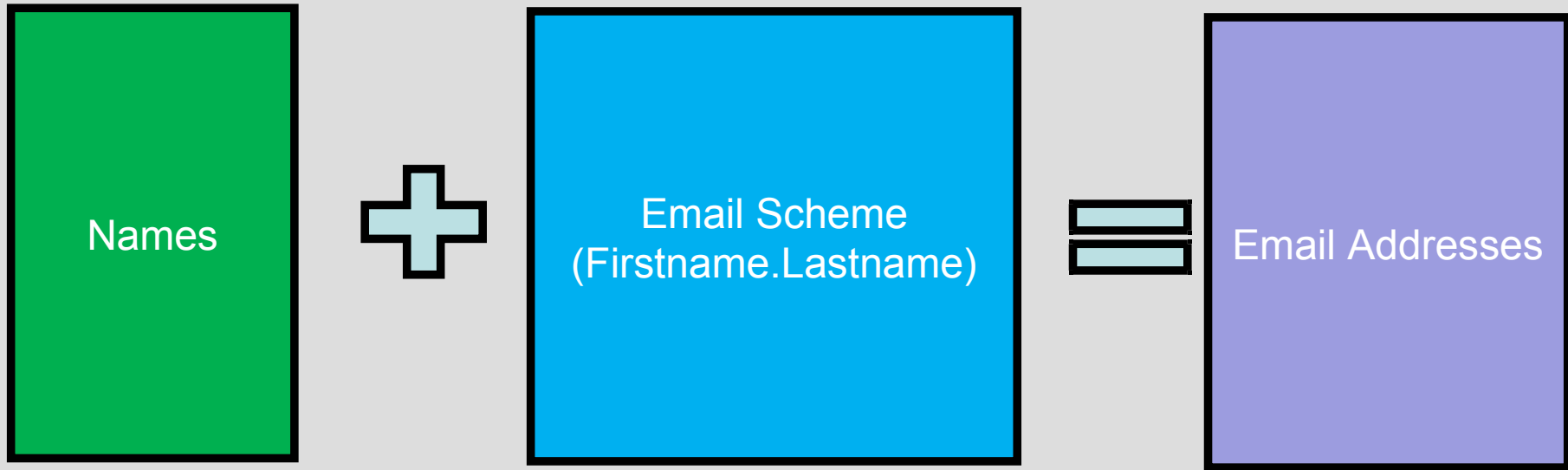
# Presentation Agenda


- Introduction
- Details of Cross Site Scripting
- [Explaining the Attack Vector](#)
- Demo
- Conclusion

# Gathering Email Address

- Company Information Websites
  - LinkedIn, Spoke and Lead411 etc
  - All are free.
- GnuPGP/PGP Keys
  - \$ ./pgp\_email\_search.pl DOMAIN.com  
(Open <http://pgp.mit.edu> Search: DOMAIN.com)
- Predictable Email addresses
  - (First.Last@Domain)

# Method to Generate Emails





John Smith  
Henry Hill



Email Scheme  
(Firstname.Lastname@COMPANY.com)



john.smith@COMPANY.com  
henry.hill@COMPANY.com



# Utilizing as an Attack Vector

- Client Base attack:
  - Phishing & Spear Phishing
- Exploit of Trust
- Vulnerabilities
  - Your website
  - Your company website
  - Websites that you and your employees trust

# Potential Damage

- Attack vector
  - Steal cookies
  - Key logging
  - Internal Port scanning
  - Appearance of website defacement
  - Browser exploits (MoBB)
  - Steal clipboard

# Presentation Agenda

- Introduction
- Details of Cross Site Scripting
- Explaining the Attack Vector
- [Demo](#)
- Conclusion

# BeEF Demo

# Presentation Agenda

- Introduction
- Details of Cross Site Scripting
- Explaining the Attack Vector
- Demo
- [Conclusion](#)

# Conclusion

- Remediation
  - Input Validation
  - Output Validation
- Software Development Life Cycle
- Questions